1988

On the Applications of Multi-Equational Resultants

Chanderjit Bajaj

Thomas Garrity

Joe Warren

Report Number:
88-826

ON THE APPLICATIONS OF MULTI-EQUATIONAL RESULTANTS

Chandrajit Bajaj
Thomas Garrity
Joe Warren

CSD-TR-826
November 1988

On the Applications of Multi-equational Resultants

Chanderjit Bajaj*
Department of Computer Science
Purdue University
West Lafayette, IN 47907

Thomas Garrity
Department of Mathematics
Rice University
Houston, TX 77251

Joe Warren†
Department of Computer Science
Rice University
Houston, TX 77251

November 29, 1988

Abstract

Computational methods for manipulating sets of polynomial equations are becoming of greater importance due to the use of polynomial equations in geometric modeling. Recently, the technique of Gröbner bases has received much attention as an algorithmic method for determining properties of systems of polynomial equations. Gröbner bases provide a method for testing ideal membership, a problem whose solution requires running time double exponential in the number of indeterminates (in the worst case). Another lesser known technique based on classical algebraic geometry is that of multi-equational resultants. Computing the resultant of several equations can be done in time single exponential in the number of indeterminates of the equations.

In this paper, we survey a range of geometric and algebraic problems that may be solved using multi-equational resultants. These problems include converting from the parametric form to the implicit form of curves and surfaces, computing the intersection of three or more surfaces, and computing the convolution of algebraic curves and surfaces. We also review a method using multi-equational resultants for decomposing an algebraic set into its irreducible components. Finally, we give an original method for computing the image of a hypersurface under a rational map and inverting this map if its is one-to-one.

*Supported in part by NSF grant MIP 85-21356, ARO contract DAAG29-85-C-0018 under Cornell MSI and ONR contract N00014-88-K-0402

†Supported in part by NSF grant IRI 88-10747

1 Introduction

Current research in geometric modeling is engaged in extending the geometric coverage of solid modelers using polynomial equations of arbitrarily high degree. Effectively manipulating these geometric representations require the ability to manipulate the underlying systems of equations [Bajaj 88]. One computational method for manipulating systems of equations is that of Gröbner bases [Buchberger 85]. Given a set of polynomials $S = \{S_1, ..., S_m\}$, Gröbner bases provide a deterministic method for determining whether a polynomial P lies in the set of all polynomials of the form $\sum A_i S_i$ (the *ideal* of S). Geometric problems such as intersection are then posed in an ideal-theoretic form and solved using Gröbner bases. One of the main difficulties involved in using Gröbner bases is that the method may be extremely slow for even small problems. In the worst case, this method requires exponential space and may have running time that is double exponential in the number of variables in problem [Mayr 82]. Even in special cases where this double exponential behavior is not observed, deriving tight upper bounds on the methods running time is difficult.

In this paper, we present an alternative method for answering a wide range of questions dealing with the *zero sets* of polynomial equations. This method is the generalization of the two equation resultant of Sylvester (see [Lang 71], section V.10) to three or more equations. Specifically, given n homogeneous equations in n variables, there exist a homogeneous polynomial in the coefficients of the equations that evaluates to zero if and only if the original equations have a common root. We refer to this polynomial as the multi-equational resultant (as distinguished from the two equation, multivariate resultant in Collins [Collins 71]).

Mathematical characterizations of the multi-equational resultant appeared in classical algebraic geometry from the late 1800's to the early 1900's. In particular, [Cayley 1848], [Macaulay 02] and [Hurwitz 13] have each suggested mathematical characterizations of the multi-equational resultant. Renewed interest in classical algebraic geometry techniques [Sederberg 86] has lead to more computational treatments of multi-equational resultants. These works include [Bajaj 87, Canny 88b].

In Section 2, we review a mathematical characterization of the multi-equational resultant by Macaulay [Macaulay 02]. A method of [Canny 88b] based on this characterization for computing the resultant in time single exponential in the number of equations, is also outlined. We next survey applications of multi-equational resultants in computing with solution sets to polynomial equations. Some of these have been presented in prior papers, however we include them here for sake of completeness. In Section 3, we show how to the use the resultant to compute the convolution of plane curves as well as the common tangent between plane curves. These operations arise in motion planning and computations with planar geometric models. In Section 4, the resultant is used to compute the implicit equations and the inverse of the rational parametric equations of a parametric surface, as well as the convolution of two parametric surfaces. We also present a way of obtaining a birational planar projection of the intersection curve of two parametric surfaces.

All these problems arise in computing boolean set and sweep operations on solid models with parametric surface boundaries.

In Section 5, the resultant is used for determining whether there is a curve singularity on an algebraic surface, for computing the convolution of two algebraic surfaces and computing the intersection of three algebraic surfaces. In Section 6, we discuss the use of the multi-equational resultant in computing the decomposition of general algebraic sets into irreducible components. We include original work on using resultants to compute the image of a hypersurface under a rational map and determine whether that map is one-to-one almost everywhere. If the map is birational, we then show that a variant of the resultant and Cramer's rule can be used to compute the inverse map. Finally, we conclude by comparing and contrasting the methods of Gröbner bases and multi-equational resultants.

2 Multi-equational Resultants

A *homogeneous* polynomial is a polynomial in which all terms are of the same degree. The zero set of a homogeneous polynomial in n variables defines a hypersurface in n dimensional *affine* space. However, if we map lines through the origin in this n dimensional space to points in a $n-1$ dimensional *projective* space, then the zero set of a homogeneous polynomial also maps to a hypersurface in the $n-1$ dimensional projective space. (See [Hartshorne 77, Chapter 1] for a more complete explanation.)

If $f_1 = 0, ..., f_n = 0$ are homogeneous polynomial equations in n variables, then the *resultant* $R(f_1, ..., f_n)$ is a polynomial in the *coefficients* of the f_i that vanishes if and only if the f_i have a common zero in projective space. For this reason, the resultant is also often called the eliminant. Geometrically, the resultant vanishes if and only if the n hypersurfaces $(f_i = 0)$ have a common intersection in projective space.

The resultant of several equations has several different characterizations. Probably the most elegant was discovered by Macaulay [Macaulay 02]. He shows that the multi-equational resultant can be expressed as the quotient of the determinant of two matrices whose entries are coefficients of the polynomials. In the case of two equations, the matrix for the denominator always has determinant 1 and the matrix for the numerator is the traditional Sylvester matrix.

In computing the multi-equational resultant, the f_i are multiplied by suitable monomials to transform the problem of determining whether the polynomials have a common zero into a problem in linear algebra. We construct a matrix whose entries are the coefficients of the $f_1, ..., f_n$. The determinant of this matrix will be the product of the resultant and the determinant of a specific minor of the matrix.

2.1 An Example

Since the construction is rather complicated, we now begin an example. Let

$$\begin{aligned} f_1 &= a_1x_1 + a_2x_2 + a_3x_3 &&= 0 \\ f_2 &= b_{11}x_1^2 + b_{12}x_1x_2 + b_{22}x_2^2 + b_{13}x_1x_3 + b_{23}x_2x_3 + b_{33}x_3^2 &&= 0 \\ f_3 &= c_{11}x_1^2 + c_{12}x_1x_2 + c_{22}x_2^2 + c_{13}x_1x_3 + c_{23}x_2x_3 + c_{33}x_3^2 &&= 0 \end{aligned}$$

be three homogeneous polynomial equations in which the coefficients are treated symbolically.

Now consider the following ten polynomials

$$x_1^2f_1, x_1x_2f_1, x_1x_3f_1, x_2^2f_1, x_3^2f_1, x_2x_3f_1, x_2f_2, x_3f_2, x_2f_3, x_3f_3. \tag{1}$$

All ten of these polynomials have degree three. Setting all of these polynomials to be zero simultaneously yields a matrix equation of the form:

$$\begin{pmatrix} a_1 & a_2 & a_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_1 & 0 & a_2 & 0 & a_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_1 & 0 & a_3 & a_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_1 & 0 & 0 & a_2 & a_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_1 & 0 & 0 & 0 & a_2 & a_3 \\ 0 & 0 & 0 & 0 & 0 & a_1 & 0 & a_2 & a_3 & 0 \\ 0 & b_{11} & 0 & b_{12} & 0 & b_{13} & b_{22} & b_{23} & b_{33} & 0 \\ 0 & 0 & b_{11} & 0 & b_{13} & b_{12} & 0 & b_{22} & b_{23} & b_{33} \\ 0 & c_{11} & 0 & c_{12} & 0 & c_{13} & c_{22} & c_{23} & c_{33} & 0 \\ 0 & 0 & c_{11} & 0 & c_{13} & c_{12} & 0 & c_{22} & c_{23} & c_{33} \end{pmatrix} \begin{pmatrix} x_1^3 \\ x_1^2x_2 \\ x_1^2x_3 \\ x_1x_2^2 \\ x_1x_3^2 \\ x_1x_2x_3 \\ x_2^3 \\ x_2^2x_3 \\ x_2x_3^2 \\ x_3^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{2}$$

The symbolic coefficients form a ten by ten matrix, A.

If f_1, f_2, and f_3 simultaneously vanish at some point in projective space, then there is some nonzero vector in the kernel of A. Thus, the determinant of A must vanish. Since the resultant vanishes if and only if f_1, f_2 and f_3 have a common solution, the resultant must be a factor of the determinant of A_{33}. To compute the resultant from A, we must still eliminate the extraneous factors in $det(A)$.

Using Macaulay's construction, this extraneous factors is the determinant of a minor of A. Eliminate from A all columns corresponding to monomials that are divisible by only one of the monomials in the set $\{x_1, x_2^2, x_3^2\}$. Next, eliminate a row if it contains an a_1, b_{22}, or c_{33} in an eliminated column. This leaves a two by two minor of A, denoted by B,

$$B = \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix}. \tag{3}$$

In this case, the resultant is exactly:

$$R = \frac{det(A)}{det(B)}.$$

2.2 The General Construction

We now state the general construction due to [Macaulay 02]. Since Macaulay's notation is difficult to understand, we use instead the notation of [Canny 88b]. Let $f_1 = 0$, ..., $f_n = 0$ be homogeneous polynomial equations in x_1, ..., x_n with f_i being of degree d_i. The coefficients of the f_i's are treated as indeterminates. Let

$$d = 1 + \sum(d_i - 1).$$

We let the n-vector α denote the exponents of a monomial in x_1, ..., x_n. For example, if $\alpha = (\alpha_1, ..., \alpha_n)$, then

$$x^\alpha = x_1^{\alpha_1} ... x_n^{\alpha_n}.$$

Thus, the set of all monomials of degree d in n variables is

$$X^d = \{x^\alpha | \alpha_1 + ... + \alpha_n = d.\}$$

If N denotes the number of monomials in this set, then the monomials will index the columns of an N by N matrix. In terms of the previous example, $d = 3$, $N = 10$ and X^3 is the set of all monomials of degree three in three variables.

We next partition X^d into n disjoint sets. These sets are

$$X_i^d = \{x^\alpha | \alpha_i \geq d_i \text{ and } \alpha_j < d_j \ , \forall j < i\}.$$

In the example, we would have

$$\begin{aligned} X_1^3 = &\ \{x_1^3, x_1^2 x_2, x_1^2 x_3, x_1 x_2^2, x_1 x_3^2, x_1 x_2 x_3\} \\ X_2^3 = &\ \{x_2^3, x_2^2 x_3\} \\ X_3^3 = &\ \{x_2 x_3^2, x_3^3\} \end{aligned}$$

Next, for each set X_i^d, we construct a set F_i of polynomials from f_i using monomials in X_i^d. Specifically, we let

$$F_i = \frac{X_i^d}{x_i^{d_i}} f_i.$$

The F_i are sets of homogeneous polynomials in n variables of degree d. Moreover, each of the polynomials in the union of the F_i, equated to zero, collectively yields a set of N homogeneous polynomial equations. Referring to the previous example, the union of F_1, F_2 and F_3 is exactly the set of polynomials in (1).

We now construct an N by N matrix (call it A) whose columns are indexed by monomials in X^d and whose rows correspond to the polynomials in the F_i's. For a given polynomial p in F_i, its row consists of the symbolic coefficients of each monomial in p. In the previous example, the matrix in equation 2 is this matrix A. Now, if the f_i have a common root $(\hat{x}_1, ..., \hat{x}_n)$, then this

root must satisfy all of the polynomial equations in the F_i's. This fact implies that the nontrivial vector $(\hat{x}_1, ..., \hat{x}_n)$ must be in the null space of A. Thus, A must be singular or equivalently, the determinant of A (call it D) must be zero. This argument establishes that the resultant R is a factor of D.

The remaining factors of D are extraneous and have no bearing on whether the original equations have a common root. The beauty of Macaulay's result is that he established that the extraneous factors are the determinant of a *minor* of A. This minor (call it B) can be constructed from A in the following manner. Delete all columns of A that correspond to monomials x^α where $\alpha_i < d_i$ for all but one value of i. (Note there must at least one such i due to the manner in which d was chosen.) Delete all rows of A that correspond to polynomials in F_i whose multipliers x^α have $\alpha_j < d_j$ for $i < j \leq n$. One consequence of this construction is that all rows corresponding to polynomials in F_n are deleted.

In the previous example, all columns except those corresponding to the monomials $x_1x_2^2$ and $x_1x_3^2$ were deleted. Likewise, all polynomials except those in F_1 multiplied by x_2^2 and x_3^2 were deleted. The resulting minor was that of equation 3.

Macaulay shows that the resultant R satisfies

$$R = \frac{det(A)}{det(B)} \tag{4}$$

where this division is carried out before the indeterminates forming the entries of A and B are specialized. The reason for specializing after division is that $det(A)$ and $det(B)$ may evaluate to zero even though R is not identically zero. A solution to this problem is presented in the next section.

2.3 Characteristic Polynomials and Affine Computations

Carrying out this symbolic division is a massive task that requires time double exponential in the number of indeterminates. To avoid this intensive computation, we now explain the method of generalized characteristic polynomials due to [Canny 88b], which also allows for specializations of the coefficient entries of matrix A.

Define new homogeneous polynomials

$$\hat{f}_i = f_i - \lambda x_i^{d_i}$$

and consider the Macaulay resultant of the polynomial equations $\hat{f}_i = 0$. After performing the matrix construction for the $\hat{f}_i$, as outlined before, one observes that the only differences are the λ appearing solely along the diagonals of the resulting matrices $\hat{A}$ and $\hat{B}$. The determinants of these new matrices are thus the characteristic polynomials of the matrices originally constructed. That is,

$$det(\hat{A}) = det(A - \lambda I) = CharPolyA(\lambda).$$

Similarly, $det(\hat{B}) = CharPolyB(\lambda)$.. Thus, the determinant of these matrices may be viewed as polynomials in λ, where the leading term of $CharPolyA$ is λ^N and the leading term of $CharPolyB$ is λ^{N-D}, with $D = \sum_{i=1}^{n} \prod_{j \neq i} d_j$. Finally,

$$R(\lambda) = \frac{CharPolyA(\lambda)}{CharPolyB(\lambda)}$$

is a polynomial of degree D.

Using the fact that a quotient polynomial of degree D, depends only on the D most significant coefficients of the divisor and dividend polynomials, $R(\lambda)$ can be computed from only the first D coefficients of both $CharPolyA(\lambda)$ and $CharPolyB(\lambda)$, yielding an efficient algorithm which is single exponential in the number of indeterminates of the original equations. Furthermore, the symbolic coefficients of the orginal f_i, the a's, b's and c's in matrix A, can now clearly be specialized to their true values (possibly constants or polynomials in other variables), with the original resultant R being recovered as the smallest non-zero coefficient of $R(\lambda)$.

One additional advantage is gained by computing resultants via the method of characteristic polynomials. In many applications, as we shall see later in Sections 3 to 6, we need to compute the multi-equational resultant for $non - homogeneous$ polynomial equations $g_i = 0$. It is possible to homogenize the polynomials g_i by introducing an additional variable, say w. Let f_i denote the homogeneous polynomials obtained from g_i in this way. While the common solutions of $f_i = 0$ for $w = 1$ correspond to the original common solutions of $g_i = 0$, there are extraneous common solutions introduced into the homogenous system $f_i = 0$ for $w = 0$ which do not correspond to any solutions of $g_i = 0$. This problem becomes acute when the dimension of the common solutions of f_i for $w = 0$ is higher than the dimension of the common solutions of $g_i = 0$, and causes a naiive multi-equational resultant computation to vanish identically.

For example, if the $g_i = 0$ are m non-homogeneous polynomial equations in n variables, then their solution set is of dimension $\geq n - m$. The solution components of dimension $= n - m$ are *proper* while the components of dimension $\geq n - m$ are *excess*. The multi-equational resultant of the homogenized polynomial system $f_i = 0$ (derived from the $g_i = 0$) is a projection into a space of dimension $n - m + 1$, yielding a hypersurface H. The *proper* dimension solutions of $g_i = 0$ can be recovered from the hypersurface H. However, if the extraneous solutions corresponding to $w = 0$ are of *excess* dimension, then the resultant would vanish identically, viz. the projection is a trivial hypersurface covering the entire $n - m + 1$ dimensional space. Fortunately, as proved by [Canny 88b], computing resultants via the method of characteristic polynomials, introduces a λ perturbation on the solution components corresponding to $w = 0$, causing all *excess* dimension components to "break up" thereby allowing one to recover the *proper* dimension solutions from a non-trivial hypersurface H.

Given the ability to compute the resultants of several homogenous or non-homogeneous equations, we next survey a range of techniques, using these multi-equational resultants, for computing

about systems of polynomial equations arising from diverse applications.

3 Applications for Algebraic Plane Curves

An algebraic plane curve is implicitly defined by a single polynomial equation $f(x,y) = 0$. A subclass of algebraic curves known as rational curves, have an alternate representation in terms of rational functions, $x = f(t)/h(t)$ and $y = g(t)/h(t)$, with f, g, h being polynomials in t.

In the following we consider both the internal representations of algebraic curves, i.e., whether they are parametrically or implicitly defined. All polynomials are assumed to be defined over an algebraically closed field such as the complex numbers. We additionally use the following notation. Partial derivatives are written by subscripting, for example, $f_x = \partial f/\partial x$, $f_{xy} = \partial^2 f/(\partial x \partial y)$, and so on. Since we consider algebraic curves and surfaces, we have $f_{xy} = f_{yx}$ etc. Derivatives of polynomials in one variable are written with primes, for example, $c'(t) = d\ c/d\ t$.

3.1 Convolution of Two Plane Curves

In [Bajaj 88b] this convolution operation is used to generate the boundary of configuration space obstacles, in order to construct collision free motion paths for translating objects.

Theorem 1 *Let C_A and C_B be two algebraic plane curves defined implicitly by $f(x,y) = 0$ and $g(\alpha,\beta) = 0$, respectivley. Then Convolution(C_A, C_B) is the set of points $\hat{p} = (\hat{x},\hat{y})$ such that*

$$\begin{aligned} \hat{x} - x - \alpha &= 0 \\ \hat{y} - y - \beta &= 0 \\ f(x,y) &= 0 \\ g(\alpha,\beta) &= 0 \\ h(x,y,\alpha,\beta) = f_x \cdot g_\beta - f_y \cdot g_\alpha &= 0 \end{aligned}$$

A proof of the above theorem can be found in [Bajaj 88b]. We can obtain an implicit polynomial equation for *Convolution*(C_A, C_B) by using the above Theorem and the multi-equational resultant as follows: First substitute $x = \hat{x} - \alpha$ and $y = \hat{y} - \beta$ in the above equations, yielding the three non-homogeneous polynomial equations

$$\begin{aligned} \hat{f}(\hat{x},\hat{y}) &= 0 \\ \hat{g}(\alpha,\beta) &= 0 \\ \hat{h}(\hat{x},\hat{y},\alpha,\beta) &= 0 \end{aligned}$$

The above system can be transformed into three homogenous polynomial equations in α, β and an additional variable γ. The multi-equational resultant is then computed from this, as detailed in 2.3,

eliminating variables α, β and γ, and yielding the $Convolution(C_A, C_B)$, a polynomial equation in $\hat{x}, \hat{y}$.

Theorem 2 *Let C_A and C_B be two rational algebraic curves defined parametrically by $(c_1(s), c_2(s))$ and $(\hat{c}_1(t), \hat{c}_2(t))$ respectively. Then $Convolution(C_A, C_B)$ is the set of points $\bar{p} = (\hat{x}, \hat{y})$ such that*

$$\begin{aligned} \hat{x} - c_1(s) - \hat{c}_1(t) &= 0 \\ \hat{y} - c_2(s) - \hat{c}_2(t) &= 0 \\ f(s,t) = c_1'(s) \cdot \hat{c}_2'(t) - c_2'(s) \cdot \hat{c}_1'(t) &= 0 \end{aligned}$$

A proof of the above theorem can again be found in [Bajaj 88b]. The implicit polynomial equation for $Convolution(C_A, C_B)$ is computed by transforming the above three equations into a homogenous polynomial system in s, t and an additional variable u, and then computing the multi-equational resultant, eliminating these variables s, t, u.

3.2 Common Tangent between Two Plane Curves

In [Bajaj 88d] the common tangent computation is used to construct the convex hull of a planar geometric model with algebraic curve boundaries. Suppose L is a common tangent between two algebraic plane curves C_A and C_B. Then the tangent points $p = (x, y)$ and $q = (\alpha, \beta)$ of L at C_A and C_B respectively are given by the following Theorem.

Theorem 3 *(I) If C_A and C_B are defined parametrically as $(x(s), y(s))$ and $(\alpha(t), \beta(t))$ respectively, then $p = (x(s), y(s))$ and $q = (\alpha(t), \beta(t))$ are given by*

$$\begin{aligned} f(s,t) = (x(s) - \alpha(t)) \cdot y'(s) - (y(s) - \beta(t)) \cdot x'(s) &= 0 \\ g(s,t) = (x(s) - \alpha(t)) \cdot \beta'(t) - (y(s) - \beta(t)) \cdot \alpha'(t) &= 0 \end{aligned}$$

(II) If C_A is defined parametrically as $(x(s), y(s))$ and C_B is defined implicitly as $f(\alpha, \beta) = 0$, then $p = (x(s), y(s))$ and $q = (\alpha, \beta)$ are given by

$$\begin{aligned} f(\alpha, \beta) &= 0 \\ g(s,t) = (x(s) - \alpha) \cdot y'(s) - (y(s) - \beta) \cdot x'(s) &= 0 \\ h(s,t) = (x(s) - \alpha) \cdot g_\alpha + (y(s) - \beta) \cdot g_\beta &= 0 \end{aligned}$$

(III) If C_A and C_B are defined implicitly as $f(x, y) = 0$ and $g(\alpha, \beta) = 0$, then $p = (x, y)$ and $q = (\alpha, \beta)$ are given by

$$
\begin{aligned}
f(x,y) &= 0 \\
g(\alpha,\beta) &= 0 \\
h(x,y,\alpha,\beta) = (x-\alpha)\cdot f_x + (y-\beta)\cdot f_y &= 0 \\
k(x,y,\alpha,\beta) = (x-\alpha)\cdot g_\alpha + (y-\beta)\cdot g_\beta &= 0
\end{aligned}
$$

A proof of the above theorem can be found in [Bajaj 88d]. The method to be used here is popularly known as the U-resultant technique [Waerden 50]. Each of the above polynomial equations are homogenized, using an additional variable w. Next a homogeneous linear equation is taken, viz., $U = u_1 s + u_2 t + u_3 w$ for (I), $U = u_1 s + u_2 \alpha + u_3 \beta + u_4 w$ for (II), and $U = u_1 x + u_2 y + u_3 \alpha + u_4 \beta + u_5 w$ for (III), involving new indeterminates u_1, u_2, u_3, u_4, u_5, in general. Next for each of the homogenous systems obtained from (I), (II) and (III) the appropriate U polynomial is added, and the multi-equational resultant computed, as detailed in 2.3. The resulting polynomial in the new indeterminates, in each of the three cases (I), (II), (III), decomposes into linear factors from which the coordinates of the common tangens points can be reconstructed. See [Canny 88a] where details are given for U-resultant polynomial computations.

4 Applications for Parametric Surfaces

An algebraic surface defined by parametric equations

$$
\begin{aligned}
x &= \frac{g_1(s,t)}{d(s,t)} \\
y &= \frac{g_2(s,t)}{d(s,t)} \\
z &= \frac{g_3(s,t)}{d(s,t)}
\end{aligned} \tag{5}
$$

is also known as a parametric surface. Parametric surfaces play a large role in Computer-Aided Geometric Design (CAGD). (See [Boehm 84] for more details). Partial derivatives are again written by subscripting, such as, $f_x = \partial f / \partial x$, and the *gradient* of f is the vector $\nabla f = (f_x, f_y, f_z)$.

4.1 Inversion Formula for Parametric Surfaces

If the given surface parameterization 5 is one-to-one, then the rational parameterization admits an inverse rational parameterization. Precisely, there must exist rational functions of the following form.

$$
s = \frac{H_1(x,y,z)}{E(x,y,z)}
$$

$$t = \frac{H_2(x,y,z)}{E(x,y,z)}$$

These inverse equations can be computed during implicitization of the parametric surface using the multivariate resultant. Recall that the fundamental process in computing the multivariate resultant is conversion of the system of polynomial equations into a larger system of linear equations. However, solutions to systems of linear equations can be computed using Cramer's rule. We will discuss this procedure in more detail in section 6.2.

These equations are particularly useful in manipulations involving parametric surface patches. For example, testing whether a point $\hat{P} = (\hat{x}, \hat{y}, \hat{z})$ lies inside a rectangular parametric patch corresponds to testing whether the image of $\hat{p}$ under the above equations lies inside a rectangle in the st plane.

4.2 Implicit Form for Parametric Surfaces

To construct the implicit equation $h(x,y,z) = 0$, corresponding to the parametric equations, we first homogenize those equations (5) with an additional variable u, yielding polynomial equations $f_1(s,t,u) = 0$, $f_2(s,t,u) = 0$ and $f_3(s,t,u) = 0$ below.

$$\begin{aligned} f_1(s,t,u) = \hat{d}(s,t,u)x - \hat{g}_1(s,t,u) &= 0 \\ f_2(s,t,u) = \hat{d}(s,t,u)x - \hat{g}_2(s,t,u) &= 0 \\ f_3(s,t,u) = \hat{d}(s,t,u)x - \hat{g}_3(s,t,u) &= 0 \end{aligned}$$

Then the implicit equation $h(x,y,z) = 0$ is obtained from the multi-equational resultant of the above three homogeneous equations, using the method detailed in 2.3. To see why, remember that the resultant polynomial is equal to zero if and only if $f_1(s,t,u) = 0$, $f_2(s,t,u) = 0$ and $f_3(s,t,u) = 0$ have common s, t and u solutions. Next, note that whenever the implicit equation $h(x,y,z) = 0$, there is a value for the parameters s and t that simultaneously satisfies the parametric equations (5).

Details of alternate methods for computing the implicit equations of parametric curves and surfaces, using the multi-equational resultant may be found in [Bajaj 87].

4.3 Planar Projection of the Intersection Curve of Two Parametric Surfaces

Another interesting application of birationality arises from the following theorem from algebraic geometry that states the following: any irreducible algebraic space curve is birational with an algebraic plane curve [Hartshorne 77]. (In fact, any zero set of a collection of polynomials that is irreducible is birational to the zero set of some single polynomial.) Using this fact, [Garrity 87]

suggests representing an algebraic space curve as an algebraic plane curve plus a birational map and gives an algorithm for computing such a representation.

A similar birational map can be computed for the intersection curve of two parametric surfaces with a plane projection in the parametric plane of either of the two parametric surfaces. The plane projection can be computed by the simultaneous elimination of either s and t or u and v from the three equations below.

$$\begin{aligned} \frac{g_1(s,t)}{d(s,t)} &= \frac{h_1(u,v)}{e(u,v)} \\ \frac{g_2(s,t)}{d(s,t)} &= \frac{h_2(u,v)}{e(u,v)} \\ \frac{g_3(s,t)}{d(s,t)} &= \frac{h_3(u,v)}{e(u,v)} \end{aligned}$$

4.4 Convolution of Two Parametric Surfaces

Theorem 4 *Let F_A be a parametric surface $(x(s,t), y(s,t), z(s,t))$ with gradient $F_s \times F_t$. Further let F_B be a parametric surface $(\alpha(u,v), \beta(u,v), \gamma(u,v))$ with gradient $G_u \times G_v$. Then Convolution(F_A, F_B) = the set of points $\hat{p} = (\hat{x}, \hat{y}, \hat{z})$ such that*

$$\begin{aligned} \hat{x} - x(s,t) - \alpha(u,v) &= 0 \\ \hat{y} - y(s,t) - \beta(u,v) &= 0 \\ \hat{z} - z(s,t) - \gamma(u,v) &= 0 \\ (F_s \times F_t) \times (G_u \times G_v) &= 0 \end{aligned}$$

A proof of the above theorem can be found in [Bajaj 88c]. We can obtain an implicit polynomial equation for *Convolution*(F_A, F_B) by using the Theorem and the multi-equational resultant as follows. The final vector equation above, yields two independent, polynomial equations. The entire system of equations can then be transformed into five homogenous polynomial equations in s, t, u, v and an additional variable w. The multi-equational resultant is then computed from this, as detailed in 2.3, eliminating variables s, t, u, v, w, and yielding the *Convolution*(F_A, F_B), a polynomial equation in $\hat{x}, \hat{y}, \hat{z}$.

5 Applications for Algebraic Surfaces

5.1 Criteria for Curve Singularity on an Algebraic Surface

$$f(x,y,z) = 0$$
$$f_x(x,y,z) = 0$$

$$f_y(x,y,z) = 0$$
$$f_z(x,y,z) = 0$$

A curve singularity on the algebraic surface $f = 0$ exists if any of the multivariate resultants of the first equation with two of the remaining three, eliminating two variables, is identically zero. For then there exists a curve singularity on the algebraic surface. The resultant being identically zero corresponds to the space curve singularity covering the entire line onto which the projection is being computed. More details are given in section 5.3.

5.2 Convolution of Two Algebraic Surfaces

In [Bajaj 88c] this convolution operation is used to generate the boundary of configuration space obstacles in space, in order to construct geodesic paths for two objects moving in contact with each other (compliant motion).

Theorem 5 *Let F_A be an algebraic surface $f = 0$ with gradient ∇f. Further let F_B be an algebraic surface $g = 0$ with gradient ∇g. Then Convolution(F_A, F_B) = the set of points $\hat{p} = (\hat{x}, \hat{y}, \hat{z})$ such that*

$$\begin{aligned}
\hat{x} - x - \alpha &= 0 \\
\hat{y} - y - \beta &= 0 \\
\hat{z} - z - \gamma &= 0 \\
f(x,y,z) &= 0 \\
g(\alpha,\beta,\gamma) &= 0 \\
\nabla f \times \nabla g &= 0
\end{aligned}$$

We use the above Theorem as follows. Using the first three equations above, substitute $x = \hat{x} - \alpha$, $y = \hat{y} - \beta$ and $z = \hat{z} - \gamma$ in the last three equations, noting that the final vector equation $\nabla f \times \nabla g = 0$ above, yields two independent polynomial equations. The entire system of equations can then be transformed into four homogenous polynomial equations in α, β, γ and an additional variable w. Next the multi-equational resultant is computed, eliminating variables α, β, γ, w, and yields the implicit equation for *Convolution*(F_A, F_B), in terms of $\hat{x}, \hat{y}, \hat{z}$.

5.3 Intersection of Three Algebraic Surfaces

Consider three implicitly defined surfaces of the form

$$F(x,y,z) = 0$$
$$G(x,y,z) = 0$$
$$H(x,y,z) = 0$$

If we eliminate x and y from these equations simultaneously using the multi-equational resultant, then resulting equations is of the form

$$R(z) = 0.$$

If R is identically zero, then the three surfaces intersect in a common space curve. If R is not identically zero, then the solutions to this equation are exactly the z coordinates of the intersection points of the three original surfaces. (Remember three surfaces in three dimensional *projective* space must always intersect in at least three points.) There are several problems with this simple approach.

First, we must recover the x and y coordinates for a specific z coordinate. Second, the intersection points may have the same z coordinate. Each of these problems is easily solved using the following observations. Taking the multi-equational resultant of the three equations is equivalent to projecting the intersection points of the three surfaces down onto a line. If we choose our direction of projection to be sufficiently generic (for example, project using an indeterminate direction), then each intersection point will project down to a unique point. Moreover, the points of projection will be *birational* with the original intersection points. (For a definition of birationality, see the next section.) This birational map can be computed using techniques similar to those in [Abhyankar 87, Garrity 87]. After computation of the points of projection (e.g. solving a univariate polynomial), the original intersection points may be computed using the birational map.

6 Applications for Algebraic Sets

The set of solutions to a collection of polynomial equations

$$f_1(x_0, ..., x_n) = 0,$$

$$...$$

$$f_m(x_0, ..., x_n) = 0,$$

is referred to as an *algebraic set*. Algebraic sets play a fundamental role in algebraic geometry. Algorithms for manipulating algebraic sets are crucial components for systems for deciding existential and universal theories of polynomial equations [Canny 88a].

6.1 Decomposing Algebraic Sets

An algebraic set that cannot be represented as the union of two other distinct algebraic sets, neither containing the other, is said to be *irreducible*. Any algebraic set can be represented as the union of distinct algebraic sets. Unfortunately, representing an algebraic set as the solution to a system of equations is often not a computationally convenient representation. However, a classical theorem from algebraic geometry provides for an alternate representation. The theorem

states that any irreducible algebraic set is birational with a hypersurface of appropriate dimension ([Hartshorne 77], Prop.I.4.9).

This theorem suggests the following problem: Given an algebraic set S, decompose S into its irreducible components C_i and construct the a hypersurface and rational map for each C_i as suggested by the theorem. This construction can be done using multi-equational resultants. Given m equations in n variables, let S be the algebraic set of dimension $n-m$ defined by these equations. We may construct a *generic* linear projection onto $n-m+1$ of the variables. The image of this projection is the zero set of a polynomial R in these $n-m+1$ variables.

Now, R is exactly the multi-equational resultant of the m original equations and the $n-m+1$ projection equations. Moreover, the irreducible factors of R over the complexes are birational with irreducible components of S. The inverse rational map from the irreducible factors of R to the C_i's may be recovered using the Theorem of the Primitive Element ([Zariski 58], section II.9).

This construction for $m=2$ is described in [Abhyankar 87, Garrity 87]. A more general version for unrestricted m is described in [BCGW 88] that also handles the case in which the dimension of S is unrestricted. Using multi-equational resultants, this algorithm runs in time single exponential in m and n.

6.2 Inverting Rational Maps

A map of the form

$$y_1 = \psi_1(x_0, x_1, ..., x_m)y_0$$

$$...$$

$$y_n = \psi_n(x_0, x_1, ..., x_m)y_0,$$

where the $\psi_i = \frac{s_i(x_0,...,x_n)}{t_i(x_0,...,x_n)}$ are ratios of homogeneous polynomials of equal degree in the x_j is referred to as a *rational* map. In general, a rational map may be thought of as a function that transforms some set of points X in $(x_0...x_m)$ space to set of points Y in $(y_0...y_n)$ space. Note that the denominators are polynomials and can have zeros. Thus the map may not be defined at all points. We denote this map by $\psi : X \rightarrow Y$.

A rational map $\psi : X \rightharpoonup Y$ is called *birational* if it admits an inverse. That is, there exists a rational map $\phi : Y \rightharpoonup X$ such that $\psi(X)$ is dense in Y (they have the same dimension), $\phi(Y)$ is dense in X, $\psi\phi = 1$ almost everywhere , and $\phi\psi = 1$ almost everywhere. Two sets X and Y are said to be *birational* if there exists a birational map between X and Y.

The parametric definition of a curve or surface is standard example of a rational map. Inverting a parametrization of a surface has applications in areas such as sorting points along a parametric curve [Johnstone 87]. Birational maps have been used in resolving the singular (nonsmooth) points of algebraic curves and surfaces [Abhyankar 88]. In particular, [Bajaj 88a] uses this idea

in the robust tracing of algebraic plane curves. Abhyankar and Bajaj use birational maps in determining whether an algebraic space curve has a rational parameterization (see [Abhyankar 86, Abhyankar 87]). From a mathematical point of view, current attempts to classify surfaces and higher dimensional geometric objects usually are restricted to classifications up to birationality [Wilson 87].

If $\psi : X \rightarrow Y$ is a rational map and $F(x_0, ..., x_n)$ is an irreducible homogeneous polynomial with rational coefficients, we describe a method for computing the image of the hypersurface under ψ using multi-equational resultants. We also describe a method for determining whether the map is 1-1 on the hypersurface and if so, give a construction based on applying Cramer's rule for generating an inverse rational map.

In the special case of inverting a parametrization of a surface S, given by

$$x = x(s,t)$$
$$y = y(s,t)$$
$$z = z(s,t),$$

we may take the (s,t) parameter planes as being the zero set of $(u = 0)$ in (s,t,u) space and view this as an instance of the above problem. If this map is 1-1 onto S, then we can compute a rational map from S to the (s,t) parameter plane plane using the following construction.

6.2.1 Computing the True Image Variety

The rational map ψ will map almost every point of the hypersurface $(F = 0)$ to a single irreducible variety. For obvious reasons this variety is called the *true image variety*. With each $\psi_i = \frac{s_i}{t_i}$, the map ψ restricted to $((t_1 \neq 0) \cup (t_2 \neq 0) \cup ... \cup (t_n \neq 0))$ is well-defined. The true image variety is the smallest irreducible variety that contains the image of ψ restricted to $((F = 0) \cap ((t_1 \neq 0) \cup (t_2 \neq 0) \cup ... \cup (t_n \neq 0)))$.

In computing the true image variety, we must first test whether F divides any of the t_i. If so, then the true image variety is empty. Otherwise, the true image variety must be non-empty. We next compute the multi-equational resultant of $F(x_0, ..., x_n) = 0$ and the n polynomial equations

$$y_i t_i(x_0, ..., x_n) - y_0 s_i(x_0, ..., x_n) = 0$$

with respect to the variables $x_0, ..., x_n$. The resultant is a polynomial R in $y_0, ..., y_n$. Factoring this polynomial using [Kaltofen 85b] yields

$$R(y_0, ..., y_n) = \prod R_i(y_0, ..., y_n)^{n_i}.$$

If the map is finite-to-one, then the true image must be a hypersurface. This hypersurface must correspond to one of the factors R_i. The zero sets of the remaining R_i's are extraneous hypersurfaces

whose preimages under ψ lie in the poles of ψ. To determine which R_i corresponds to the true image variety, we choose a point p on $F = 0$ that does not lie on a pole of ψ (such a point exists since F does not divide any of the t_i). Now, $R_i(\psi(p)) = 0$ if and only is $R_i = 0$ is the true image variety.

6.2.2 Computing the Inverse Map

In this section we determine the degree of the rational map ψ from the hypersurface $(F = 0)$ to the true image variety, assuming of course that the map is finite-to-one. Further, if the map is generically one-to-one, which means that, under ψ, $(F = 0)$ and the true image variety are birational, we construct the inverse map. By using Macaulay's description of the resultant as the quotient of two determinants, the construction reduces to an application of Cramer's Rule.

Let $R_1(y_0, ..., y_n)$ be the irreducible factor of the resultant $R(y_0, ..., y_n)$ corresponding to the true image variety. Let k be the multiplicity of R_1 (i.e. R_1^k divides R but R_1^{k+1} does not). Then by applying ([Fulton 84],Theorem 8.4.13), we see that the map ψ from $(F = 0)$ to the true image variety $(R_1 = 0)$ is generically k to one.

If k is equal to one, then $(F = 0)$ will be birational to $(R_1 = 0)$, by:

Theorem 6 *Let X and Y be two irreducible n-dimensional varieties and ψ a rational map from X to Y that is generically one-to-one. Then under ψ, X and Y are birational.*

This follows from ([Hartshorne 77], Cor. I.4.5). We can therefore determine if $(F = 0)$ is birational to $(R_1 = 0)$ by finding the multiplicity of the factor R_1.

Assume now that the map ψ is generically one-to-one. Then, for a generic point $(y_0 : ... : y_n)$ on $(R_1 = 0)$, there is a unique point $(x_0 : ... : x_n)$ on $(F = 0)$. We want to construct the inverse map from $(y_0 : ... : y_n)$ to $(x_0 : ... : x_n)$. This construction will be reduced to a problem in matrix manipulation. Recalling equation 4, the resultant is

$$R(y_0, ..., y_n) = \frac{det(A(y_0, ..., y_n))}{det(B(y_0, ..., y_n))}.$$

where B is a specific minor of an N by N matrix A.

Now we can now apply matrix theory to A to generate an inverse rational map. Specifically, we use Cramer's rule. To apply Cramer's rule, we must first show that there exists a $(N - 1)$ by $(N - 1)$ minor of A that is non-singular.

Assume for a minute that R_1 does not divide $det(B)$. Then the order of vanishing of $det(A)$ at a generic point of $(R_1 = 0)$ must equal the order of vanishing of R. Since the map ψ is generically one-to-one, this order of vanishing must be one. Since the order of vanishing of $det(A)$ is one, the

kernel of the matrix A must be one dimensional. Recalling equation 2

$$A \begin{pmatrix} x_0^d \\ . \\ . \\ . \\ x_n^d \end{pmatrix} = \begin{pmatrix} 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}, \tag{6}$$

Thus, the vector $(x_0^d, ..., x_n^d)$ spans the kernel of A.

Since the point $(x_0 : ... : x_n)$ is in projective space, we can assume, after relabeling, that $(x_n \neq 0)$. Since the kernel of A is one-dimensional, any vector of the form $(\alpha_1, ..., \alpha_{N-1}, 0)$ cannot lie in the kernel of A. Thus,

$$A \begin{pmatrix} \alpha_1 \\ . \\ . \\ . \\ \alpha_{N-1} \\ 0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}.$$

for all possible α_i. Labeling the columns of A by A_1 through A_N, this equation may be rewritten as

$$A \begin{pmatrix} \alpha_0 \\ . \\ . \\ . \\ \alpha_{N-1} \\ 0 \end{pmatrix} = \alpha_1 A_1 + ... + \alpha_{N-1} A_{N-1} \neq \begin{pmatrix} 0 \\ . \\ . \\ . \\ 0 \end{pmatrix},$$

for all $\alpha_1, ..., \alpha_{N-1}$. Thus, the $N-1$ vectors A_1 through A_{N-1} are linearly independent and therefore there must be an invertible $(N-1)$ by $(N-1)$ minor of the matrix $(A_1, ..., A_{N-1})$. This minor will be the matrix that will be used in applying Cramer's Rule.

We now construct the actual inverse map. Using the A_i, we may rewrite equation 6 as a sum of column vectors:

$$x_0^d A_1 + ... + x_{n-1} x_n^{d-1} A_{N-1} = -x_n^d A_N.$$

Thus,

$$(A_1, ..., A_{N-1}) \begin{pmatrix} x_0^d \\ . \\ . \\ . \\ x_{n-1} x_n^{d-1} \end{pmatrix} = \begin{pmatrix} column \\ vector \\ with \\ x_n^d \\ terms \end{pmatrix}.$$

Removing a single row from the matrix $(A_1, ..., A_{N-1})$, we obtain an invertible matrix. Let A'_i denote the *ith* column of this invertible matrix. Then

$$(A'_1, ..., A'_{N-1}) \begin{pmatrix} x_0^d \\ . \\ . \\ . \\ x_{n-1}x_n^{d-1} \end{pmatrix} = \begin{pmatrix} column \\ vector \\ with \\ x_n^d \\ terms \end{pmatrix}.$$

Since $(A'_1, ..., A'_{N-1})$ is invertible, we can apply Cramer's Rule ([Herstein 75], Thm. 6.9.2) to find the inverse rational map.

There is one last technical point to resolve. We assumed that $R_1(y_0, ..y_n)$ did not divide $det(B(y_0, ..y_n))$. Unfortunately, this can happen. There is, though, a way around this problem. Recall that the construction of the matrices $A(y_0, ..y_n)$ and $B(y_0, ..y_n)$ depends on the order of the equations

$$\begin{aligned} F(x_0, ..., x_n) &= 0 \\ y_1 t_1(x_0, ..., x_n) &= y_0 s_1(x_0, ..., x_n) \\ &... \\ y_n t_n(x_0, ..., x_n) &= y_0 s_n(x_0, ..., x_n). \end{aligned}$$

Let y_i be present in a term of R. Reorder the above equations so that

$$y_i t_i(x_0, ..., x_n) = y_0 s_i(x_0, ..., x_n)$$

is the last equation. With this new ordering of the equations, reconstruct the matrices A and B. By examining how the minor B is constructed, we see that B is independent of the term y_i. Thus $R_1(y_0, ..y_n)$ cannot divide $B(y_0, ..y_n)$.

7 Multi-equational Resultants vs. Gröbner Bases

All of the above problems can be solved using multi-equational resultants. These problems can also be solved by using Gröbner bases. One simply poses the problems as ideal membership questions. Unfortunately these ideal membership questions may have solutions that require time double exponential in the number of variables [Mayr 82]. In contrast, the resultant method of [Canny 88b] has a running time that is single exponential in the number of equations being solved. One benefit of using Macaulay's formulation of the resultant is that algorithms for computing with matrices and determinants are well understood. As a result, it is often possible to state precise time bounds for problems involving multi-equational resultants. Another benefit is that the matrices produced by Macaulay's method are highly structured and should allow computation of their determinant

in time proportional to the square of their size (instead of the cube of their size using Gaussian elimination). This situation further contrasts that of Gröbner bases in which running times are related to simplification under rewrite rules. The behaviour of these rewrite procedures is difficult to establish except for special cases. These observations suggest that for computation involving the *zero sets* of polynomial equations multi-equational resultants may prove more efficient than Gröbner bases.

8 Conclusion

Two main conclusions may be drawn from this work. There exists a large body of mathematical knowledge in algebraic geometry. This knowledge could be of significant importance in solving computational problems concerning geometric models in computer aided design and computer graphics. Second, elimination methods for systems of polynomials, the cornerstone of algebraic geometry before 1940, provide a sound basis for computational methods of symbolically manipulating polynomials. Methods such as multi-equational resultants deserve further investigation.

Acknowledgements

We would like to thank John Canny for bringing Macaulay's 1902 paper on resultants to our attention. Without Macaulay's paper, this work would have been difficult. We would also like to thank Professor Shreeram Abhyankar for his discussion of rational and birational maps. His clear explanation of their mathematics has been of great use.

References

[Abhyankar 88] Abhyankar, S. (1988), "Good Points of a Hypersurface," *Advances in Mathematics*, 68, 2, 87 - 256.

[Abhyankar 86] Abhyankar, S. and Bajaj, C. (1987), "Automatic Parameterization of Rational Curves and Surfaces III: Algebraic Plane Curves", *Computer Aided Geometric Design*, 5, 309 - 321.

[Abhyankar 87] Abhyankar, S. and Bajaj, C. (1987), *Automatic Parameterization of Rational Curves and Surfaces IV: Algebraic Space Curves* , Technical Report, CSD-TR-703, Department of Computer Science, Purdue University.

[Bajaj 87] Bajaj, C. (1987), *Algorithmic Implicitization of Algebraic Curves and Surfaces*, Technical Report, CSD-TR-681, Department of Computer Science, Purdue University.

[Bajaj 88] Bajaj, C. (1987), "Geometric Modeling with Algebraic Surfaces", *The Mathematics of Surfaces III*, ed. D. Handscomb, Oxford University Press, in press.

[Bajaj 88a] Bajaj, C., Hoffmann, C., Hopcroft, J., and Lynch, R., (1988) "Tracing Surface Intersections", *Computer Aided Geometric Design*, 5, 285 - 307.

[Bajaj 88b] Bajaj, C. and Kim, M., (1988), "Generation of Configuration Space Obstacles: The Case of Moving Algebraic Curves," *Algorithmica*, in press.

[Bajaj 88c] Bajaj, C. and Kim, M., (1988), "Generation of Configuration Space Obstacles: The Case of Moving Algebraic Surfaces," *International Journal of Robotics Research*, in press.

[Bajaj 88d] Bajaj, C. and Kim, M., (1988), "Algorithms for Planar Geometric Models," *Lecture Notes in Computer Science*, 317, 67-81.

[BCGW 88] Bajaj, C., Canny, J., Garrity, T., and Warren, J. (1988), "Decomposing Algebraic Sets", in preparation.

[Boehm 84] Boehm, W., Farin, G., and Kahmann, J., (1984), A Survey of Curve and Surface Methods in CAGD, *Computer Aided Geometric Design*, 1, 1-60.

[Buchberger 85] Buchberger, B., (1985) "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory," *Multidimensional Systems Theory*, Chapter 6, N. Bose (eds). Reidel Publishing Co.

[Canny 88a] Canny, J. (1988), "Some Algebraic and Geometric Computations in PSACE," *28'th Symposium on Theory of Computing*, pp. 460-467.

[Canny 88b] Canny, J. (1988), "Generalized Characteristic Polynomials," *International Symposium on Symbolic and Algebraic Computation*, ISSAC '88, to appear.

[Cayley 1848] Cayley, A. (1848), "On the Theory of Elimination," *Cambridge and Dublin Mathematics Journal*, Vol. III, pp. 116-120.

[Collins 71] Collins, G. (1971), "The calculation of multivariate polynomial resultants", *JACM*, Vol. 18, No. 4, Oct. 1971, pp. 515-522.

[Fulton 84] Fulton, W. (1984) *Intersection Theory*, Springer-Verlag.

[Garrity 87] Garrity, T. and Warren, J. (1987), "On Computing the Intersection of a Pair of Algebraic Surfaces", *Computer Aided Geometric Design*, in press.

[Hartshorne 77] Hartshorne, R. (1977), *Algebraic Geometry*, Springer-Verlag.

[Herstein 75] Herstein, I.N. (1975) *Topics in Algebra*,second edition, John Wiley and Sons.

[Hurwitz 13] Hurwitz, A. (1913), "Uber die Tragheitsformem Anes Algebraischen Moduls," *Annali di Matemaica*, Vol. 3, No. 20.

[Johnstone 87] Johnstone, J. (1987), *The Sorting of Points Along An Algebraic Curve*, Ph.D. Thesis, Department of Computer Science, Cornell University.

[Kaltofen 85b] Kaltofen, E. (1985), "Polynomial-Time Reductions from Multivariate to Bi- and Univariate Integral Polynomial Factorization," *SIAM J. Computing*, Vol. 14, pp. 469-489.

[Lang 71] Lang, S. (1971) *Algebra*, Addison-Wesley.

[Macaulay 02] Macaulay, F. (1902), "Some Formulae in Elimination," *Proc. London Math. Soc.*, Vol. 35, pp. 3-27.

[Mayr 82] Mayr, E. and Meyer, A. (1982), "The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals," *Advances in Mathematics*, Vol. 46, pp. 305-329.

[Sederberg 86] Sederberg, T. and Goldman, R. (1986), "Algebraic Geometry for Computer-Aided Geometric Design," *IEEE Computer Graphics and Applications*, Vol. 6, No. 6, pp. 52-59.

[Waerden 50] van der Waerden, B., (1950), *Modern Algebra*, vol. II, Ungar Publishing, New York.

[Wilson 87] Wilson, P.M.H. (1987), "Towards Birational Classification of Algebraic Varieties," *Bull. London Math Soc.*, Vol. 19, pp. 1-48.

[Zariski 58] Zariski, O. and Samuel, P. (1958), *Commutative Algebra (Vol.I, II)*, Springer Verlag.